

IN THE CLAIMS

The following is a complete listing of the claims, and replaces all earlier versions and listings.

1. (Previously Presented) A method of inserting a message into digital data representative of physical quantities, the message including ordered symbols, said method comprising the steps of:

segmenting the data into regions; and

associating at least one region with each symbol to be inserted,

wherein, for each region into which a symbol in question is to be inserted, said associating step includes the steps of:

determining a pseudo-random function, from a key which depends on an initial key and on a length of the message,

modulating the symbol in question by a previously determined pseudo-random function in order to supply a pseudo-random sequence, and

adding the pseudo-random sequence to a region in question.

2. (Previously Presented) A method according to Claim 1, wherein a dependence of the key as regards the length of the message is provided by a dependence of the key as regards:

a number of times the symbol to be inserted has already been inserted into other regions, and

a ranking of the symbol among the ordered symbols.

3. (Previously Presented) A method according to Claim 1 or 2, further comprising the step of transforming the digital data by a reversible transformation.

4. (Currently Amended) A method for extracting a message from digital data representative of physical quantities, the message including ordered symbols, said method comprising the steps of:

segmenting the data into regions;

extracting a length of an inserted message based on the digital data; and

extracting the inserted message.

5. (Previously Presented) A method according to Claim 4, wherein said step of extracting the length of the inserted message includes the steps of:

selecting a set of length values;

calculating a correlation value between the message and the digital data, for each of the length values; and

determining a local maximum among the correlation values.

6. (Previously Presented) A method according to Claim 4 or 5, wherein said step of extracting the length of the inserted message is carried out while processing F times fewer coefficients than included in the digital data.

7. (Previously Presented) A method according to Claim 6, further comprising the steps of:

- determining a total number of coefficients to be considered;
- selecting a maximum number of coefficients corresponding to a same inserted symbol, and, if the total number of coefficients to be considered has not been reached,
- reiterating said selecting step, for another symbol.

8. (Previously Presented) A device for inserting a message into digital data representative of physical quantities, the message including ordered symbols, said device comprising:

- means for segmenting the data into regions; and
- means for associating at least one region with each symbol to be inserted, wherein said means for associating includes:
 - means for determining a pseudo-random function, for each region into which a symbol in question is to be inserted, from a key which depends on an initial key and on a length of the message,
 - means for modulating the symbol in question by a previously determined pseudo-random function in order to supply a pseudo-random sequence, and
 - means for adding the pseudo-random sequence to a region in question.

9. (Previously Presented) A device according to Claim 8, wherein said means for determining a pseudo-random function is configured in such a way that a dependence of the key as regards the length of the message is provided by a dependence of the key as regards:

a number of times the symbol to be inserted has already been inserted into other regions, and

a ranking of the symbol among the ordered symbols.

10. (Previously Presented) A device according to Claim 8 or 9, further comprising means for prior transformation of the digital data by a reversible transformation.

11. (Currently Amended) A device for extracting a message from digital data representative of physical quantities, the message including ordered symbols, said device comprising:

means for segmenting the data into regions;

means for extracting a length of the inserted message based on the digital data; and

means $[(23)]$ for extracting the inserted message.

12. (Previously Presented) A device according to Claim 11, wherein said means for extracting the length of the inserted message includes:

means for selecting a set of length values,
means for calculating a correlation value between the message and the
digital data, for each of the length values, and
means for determining a local maximum from among the correlation values.

13. (Previously Presented) A device according to Claim 11 or 12, wherein
said means for extracting the length of the inserted message is configured to perform
extraction while processing F times fewer coefficients than included in the digital data.

14. (Previously Presented) A device according to Claim 13, further
comprising:
means for determining a total number of coefficients to be considered;
means for selecting a maximum number of coefficients corresponding to a
same inserted symbol; and
means for reiterating processing of said means for selecting, for another
symbol, if the total number of coefficients to be considered has not been reached.

15. (Previously Presented) A device according to Claim 8, wherein said
steps of segmenting and associating, and the steps of determining, modulating, and adding
are performed by:

a microprocessor,
a read-only memory including a program for processing the data, and

a random-access memory including registers suitable for recording variables modified during running of the program.

16. (Previously Presented) A device according to Claim 11, wherein said means for segmenting and said means for extracting are incorporated into:

a microprocessor,

a read-only memory including a program for processing the data, and

a random-access memory including registers suitable for recording variables modified during running of the program.

17. (Previously Presented) An apparatus for processing a digital image, comprising means suitable for implementing the method according to any one of claims 1 and 4.

18. (Previously Presented) An apparatus for processing a digital image, comprising a device according to any one of claims 8 and 11.

19. (Previously Presented) A storage medium storing a computer-readable program for implementing a method for inserting according to Claim 1.

20. (Previously Presented) A storage medium according to Claim 19,

wherein said storage medium is detachably mountable on a device for inserting a message that includes ordered symbols into digital data representative of physical quantities, and

wherein the device comprises:

means for segmenting the data into regions;

means for associating at least one region with each symbol to be inserted, said means for associating including:

means for determining a pseudo-random function, for each region into which a symbol in question is to be inserted, from a key which depends on an initial key and on a length of the message,

means for modulating the symbol in question by a previously determined pseudo-random function in order to supply a pseudo-random sequence, and

means for adding the pseudo-random sequence to a region in question.

21. (Previously Presented) A storage medium according to Claim 19, wherein said storage medium is a floppy disk or a CD-ROM.

22. (Previously Presented) A computer program product embodying a computer program with executable instructions for causing a computer to perform a method of inserting according to Claim 1.

23. (Previously Presented) A storage medium storing a computer-readable program for implementing a method of extracting according to Claim 4.

24. (Previously Presented) A storage medium according to Claim 23, wherein said storage medium is detachably mountable on a device for extracting a message that includes ordered symbols from digital data representative of physical quantities, the device comprising:

- means for segmenting the data into regions;
- means for extracting a length of the inserted message; and
- means for extracting the inserted message.

25. (Previously Presented) A storage medium according to Claim 23, wherein said storage medium is a floppy disk or a CD-ROM.

26. (Previously Presented) A computer program product embodying a computer program with executable instructions for causing a computer to perform a method for extracting according to Claim 4.